

# Biometrics: You are your password

**DAN STRASSBERG, SENIOR TECHNICAL EDITOR**

For verifying your identity, your physical attributes are better in many ways than a password. But which attributes to use and what mass-market products should be the first to use this technology are provoking a spirited debate in the biometrics community.

.....

**B**iometrics is a hot topic. The idea of using your physical attributes—fingerprints, a voiceprint, or any of several other characteristics—to prove your identity has a lot of appeal. Passwords and personal-identification numbers (PINs) are fraught with problems. Biometrics offers solutions. Applications that are preparing to accept biometric data include computer networks, ATMs, cars, cellular phones, and dozens of other types of embedded systems.

After years of producing relatively high-priced technology for specialized—often government-funded—niches, the biometrics industry is expanding. Several companies have announced dramatically less expensive sensors that enable biometrics to target high-volume applications. Many of these devices are at least at the preproduction stage. Still, like any emerging technology, especially one based on measurements as inexact as those of human attributes, biometrics must go a long way before it fulfills its proponents' optimistic forecasts.

In the computer industry, the goal of biometrics advocates is ubiquitous deployment. Some proponents talk of attaching not just one, but several biometric sensors to every PC. Because of the prospect of selling hundreds of millions of sensors and software packages, some biometrics advocates envision the likelihood of accumulating enormous wealth.

For biometrics, widespread acceptance means use in areas that daily affect the lives of millions of people. By replacing PINs, biometric techniques can potentially pre-



**Optical fingerprint scanners no longer have to cost more than \$1000. Biometric Access Corp's SecureTouch lists for \$199. It connects to a PC's parallel port and provides a pass-through facility for other parallel-port-connected peripherals.**

## BIOMETRICS

vent unauthorized access to or fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks. For financial transactions conducted via telephone and wire, biometrics could replace PINs and

passwords. In automobiles, biometric techniques can replace keys or keyless-entry devices. In buildings and work areas, biometric techniques may replace keys, badges, and readers.

By replacing PINs for transfers of

funds to the cards, biometrics could enhance the security of credit/debit-card (plastic-money) systems and prepaid telephone calling cards. Biometric techniques might also provide security not previously envisioned for "cash"

### FINGERPRINT SENSING—POINTING THE WAY TO LOW-COST BIOMETRICS

Of all the areas of biometrics, fingerprint sensing is the one that currently appears to have captured the imagination of the largest number of companies. Four IC manufacturers embody unusual fingerprint-sensing technologies in new chips. Dozens of companies that aren't in the IC business have announced fingerprint-sensing units. Some of these units use the new IC technologies; others use optical approaches.

Although optical fingerprint sensing is not new, some of the new optics-based sensing units offer much lower prices and smaller sizes than did their predecessors. And, although they attribute these properties to advances in optical technology, the manufacturers don't reveal very much about the advances. Nevertheless, the new units' size and cost suggest that optical fingerprint sensors may be able to compete with IC sensors. Optical-sensor manufacturers also like to point out that none of the IC fingerprint sensors is yet shipping in quantity, whereas optics-based sensors have been shipping for years.

Two of the IC approaches—one from SGS-Thomson, the other from Veridicom, a spin-off of Lucent Technologies' Bell Laboratories ([www.bell-labs.com](http://www.bell-labs.com))—are dc-capacitive sensors. Harris Semiconductor Corp's FingerLoc is an ac-capacitive sensor. The fourth approach, Thomson-CSF's FingerChip, uses thermal sensing.

Like most optical fingerprint sensors, each IC sensor produces a high-resolution (several-hundred-pixels by several-hundred-pixels by 8 or 16 bits) image of a finger tip. These images are comparable with those obtained by pressing inked finger tips onto absorbent paper. In fact, automatic fingerprint-identification systems can process images obtained from biometric sensors just as easily as they can process images obtained from inked fingers.

With the sensors, however, there is no ink and no mess. In uncompressed form, the images occupy several hundred kilobytes. Many fingerprint-based authentication systems store the images in a compressed form, in which they occupy approximately 10 kbytes. Although the image compression uses lossy algorithms, the algorithms are tuned for fingerprint recognition. Most fingerprint experts say that they can't detect differences between the original and the decompressed images.

An even more compact way to store the important features of fingerprints is to extract minutiae (**Figure A**). Minutiae are the points at which fingerprint patterns branch and end. Some suppliers of software that extracts minutiae say that their software can

represent any fingerprint in 300 bytes or less. Others say that a minutiae file can occupy as much as 1200 bytes. Either way, minutiae files significantly compress the original image.

You cannot reconstruct the original image from the minutiae, however. Still, law-enforcement personnel can perform automated searches through minutiae databases to find prints that are likely to match a print recovered from a crime scene. When it identifies the database records that are likely to contain a matching print, the computer decompresses those images. (Remember, the compressed images reside in files of roughly 10 kbytes; the much smaller minutiae files contain insufficient data to re-create fingerprint images.) Experts then evaluate the decompressed images to determine the likelihood of their matching the crime-scene print.

The dc-capacitive fingerprint sensors from SGS-Thomson and Veridicom consist of rectangular arrays of capacitors on a silicon

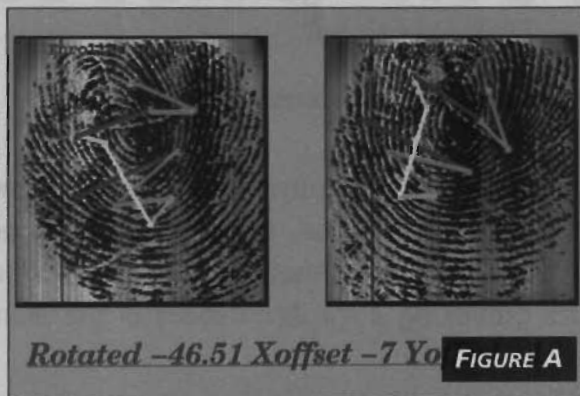
chip. One plate of the capacitor is your finger; the other plate is a tiny area of metallization (a pixel) on the chip's surface. You place your finger against the surface of the chip (actually against an insulated coating on the chip's surface). The ridges of your fingerprint are close to the nearby pixels and have high capacitance to them. The valleys are more distant from the pixels nearest them and therefore have lower capacitance.

The sensor then draws a fixed charge from each pixel in turn (that is, it scans the pixels). A high voltage appears on pixels to which your finger has low capacitance, and a low voltage appears on pixels to which your finger has a high capacitance.

SGS-Thomson's TouchChip uses an active-sensing technology in which each pixel comprises two tiny side-by-side plates (**Figure B**). Each plate is one terminal of a capacitor; your finger is the other terminal. The plate that does the sensing connects to the input of an inverter. The other plate connects to the inverter's output. The inverter acts as a buffer between its pixel and the chip's ADC. The two-capacitor architecture maintains a roughly constant average voltage on all of the pixels' plate pairs, thus minimizing the effects of parasitic capacitance.

#### Trailing-edge IC technology

One of the beauties of the dc-capacitive-sensing technology is that IC manufacturers can produce the chips with otherwise obsolete wafer-fabrication processes. No amount of improvement of



**The most compact way to store key elements of a fingerprint is as minutiae, the points at which the fingerprint patterns branch or end. Although a gray-scale fingerprint image usually occupies 100 kbytes or more, a minutiae file can occupy as little as 300 bytes (courtesy Veridicom).**

balances stored in such cards. For point-of-sale terminals, biometric techniques could replace a clerk's verification of a customer's signature.

Biometric techniques could also potentially replace driver's licenses or

passports for authenticating the identity of airline passengers. Similar techniques could replace or supplement passports and visas for establishing the identity of people seeking to cross national borders at customs and immi-

gration checkpoints.

In hospitals, biometric techniques could replace ID bracelets to establish patients' identities—for example, before blood administration. Biometrics could help confirm the identity of

IC process geometries can reduce the size of a human finger, and the chips have to be as large as a finger tip. The chips thus measure about  $12 \times 20$  mm, which is large as ICs go. But the feature size is a generous  $0.7 \mu\text{m}$ , so the large die size does not translate into unreasonable cost. Also, the defect-density requirements are modest. A chip can have a complete row of defective pixels and still work well.

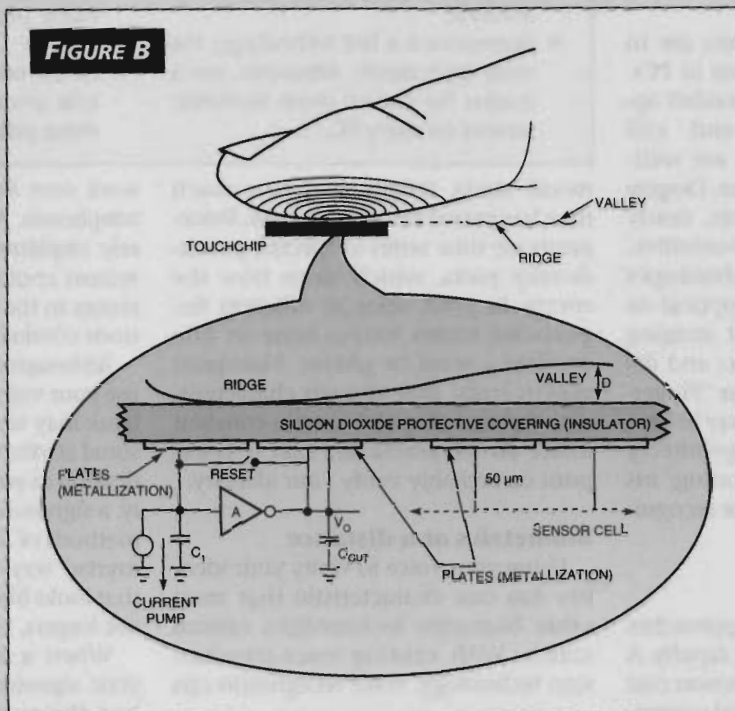
Veridicom's approach is similar to SGS-Thomson's except that Veridicom does not use an inverter per pixel. The absence of inverters makes Veridicom's chip inherently simpler than SGS-Thomson's. SGS-Thomson says, however, that the two devices are roughly equal in complexity. Also, SGS-Thomson credits the use of an inverter-per-pixel approach with the relatively easy job the company had in achieving satisfactory immunity to parasitic capacitance.

Besides dc-capacitive sensing, an IC can obtain an image of a finger tip's ridges and valleys in several ways. Harris' FingerLoc IC is also a capacitive sensor, but instead of measuring capacitance with dc, it uses an ac electric field. And, CCD optical image sensors are at the heart of most optical fingerprint sensors.

Thomson-CSF's FingerChip uses a 2-D array of semiconductor temperature sensors to capture fingerprint images. Your finger's ridges are close to the chip and thus conduct heat away more effectively than do the valleys, which are insulated by a layer of air.

The original implementation of FingerChip was a linear array of sensors. To make the device work properly, you had to draw your finger across the IC at a rather closely controlled rate. Many subjects encountered difficulty with this aspect of the device's operation. The current version uses a 2-D array. According to Thomson-CSF, although you must still draw your finger across the IC, the acceptable range of speeds is so wide that subjects no longer experience difficulty using the device. Moreover, because it takes

**FIGURE B**



**Using a cell (pixel) that comprises two capacitors and driving the second capacitor with an inverter reduce the parasitic-capacitance susceptibility of SGS-Thomson's TouchChip fingerprint-sensor IC.**

advantage of mechanical scanning (drawing the finger across the chip), FingerChip need not be as large as a finger tip.

Who? Vision Systems asserts that its TactileSense technology is less expensive than but superior to the IC manufacturers'. The technology may be a breakthrough, but the company intentionally doesn't reveal many details. According to Who? (no, this isn't an Abbott and Costello routine), TactileSense uses an electro-optical sensor chip about which the company provides few details. The chip's area is only 1% that of the direct-capacitive-sensing chips.

What enables the use of the small chip is an inexpensive, flexible polymer material. According to the company, the material focuses the finger's image onto the chip's small area. A spokesman asserts that if

you press your finger against the polymer, you can see a glowing image of your finger on the polymer surface that normally contacts the IC. The company says that you can scratch the plastic and expose it to moisture, dirt, sodium, and static electricity without affecting the sensor's operation.

Who? asserts that a complete sensing unit fits in a volume of less than 1 in.<sup>3</sup> and costs \$25 to \$50 in quantity. SGS-Thomson gives a price of less than \$50 for a complete module, including the TouchChip and a PC interface. Moreover, the company's 1-in.-sq sensor module (see the photo on pg 46) accommodates an ASIC that can perform such functions as encryption or minutiae extraction. SGS-Thomson asserts that when its competitors talk about similarly priced modules, they are talking about units that perform fewer functions—something the competitors deny.

One of Who? Vision's assertions is that because you never directly touch the chip in its device, the device is inherently more rugged than direct-capacitive-sensing devices. The IC companies disagree, however. SGS-Thomson, for example, says it has developed coatings that you can scratch with a diamond scribe without damaging the coated chip.



## BIOMETRICS

people seeking public assistance, Medicare, and other government and insurance benefits. In these applications, biometrics would replace or supplement a variety of systems, of which photo IDs are probably the most popular. Biometrics could also authenticate e-mail and other documents transmitted via computer networks. In most cases, these messages are not currently authenticated.

Many of these applications are in embedded systems rather than in PCs. Except for two types of embedded applications—automobiles and cell phones—the unit volumes are well below a million units per year. Despite the modest volumes, however, nearly all of the applications are cost-sensitive.

Some of the biometric technologies are face recognition using optical or thermal imaging; fingerprint imaging using optical, thermal and ac- and dc-capacitive sensing (see sidebar “Fingerprint sensing—pointing the way to low-cost biometrics”); hand-geometry measurement and palm scanning; iris and retina scanning; signature recognition; and voiceprints.

### Varying cost

The cost of the various approaches varies widely and is changing rapidly. A year or two ago, fingerprint sensors cost more than \$1000. Now, several companies are talking about units that cost less than \$50. Face recognition cost about \$1500 a short while ago. Now, on a PC that incorporates a desktop videocamera, the hardware is, in effect, free. The only cost is that of the software—several hundred dollars.

Voiceprint and signature-recognition equipment still costs in the neighborhood of \$1000, and equipment that measures hand geometry costs about twice as much. Iris- and retina-scanning systems cost more than \$5000. Thermal-imaging-system prices begin at about \$50,000, but that cost is for an entire enterprise. Prorated among a number of imaging stations, the costs are probably comparable with those of iris scanners.

Voiceprints and signatures are called “behavioral biometrics” because a variety of not-strictly-physical factors can affect them. These factors include

## @a glance

- Using your physical attributes to verify or authenticate your identity has many advantages over the traditional approach—passwords and PINs.
- No biometric approach is 100%-accurate.
- Biometrics is a hot technology; the most enthusiastic advocates see a market for one or more biometric sensors on every PC.
- Biometric technology must overcome many problems before it can achieve ubiquitous deployment.
- Despite enthusiasm in the PC industry, using biometrics in embedded systems makes more sense than do many proposed desktop-PC applications.
- Of the embedded applications, cellular phones appear to have enormous potential for biometrics.

mood, stress, fatigue, and how much time has passed since you awoke. Voiceprints are time series of spectral-power-density plots, which show how the energy in your voice at different frequencies varies versus time as you vocalize a word or phrase. Voiceprint experts insist that enough characteristics of your voiceprint remain constant under all circumstances that a voiceprint can reliably verify your identity.

### Biometrics at a distance

Using your voice to verify your identity has one characteristic that most other biometric technologies cannot match. With existing voice-transmission technology, voice recognition can

work over long distances via ordinary telephones. A well-conceived and properly implemented voice-based security system could provide major enhancements to the safety of financial transactions conducted over the telephone.

Although friends and associates may use your voice to identify you, and your bank may someday do likewise, no personal attribute is as common for identification as your signature. Unfortunately, a signature is one of the least reliable methods of identification. Forgers have myriad ways of producing a signature that looks like yours. Biometrics can foil the forgers, however.

When a biometric sensor captures your signature, it captures more than just the appearance of your writing. Someone who forges your signature does not necessarily make the various pen strokes the same way you do. A biometric signature-capture unit measures such variables as the speed and direction of your hand movements as you form your signature. Some units also measure the force with which you press the pen against the paper and the angle at which you hold the pen. The units often consist of a pad that contains a resistive grid or a 2-D array of ultrasonic sensors. One unit, LCI Computer Group's Smartpen, includes a group of sensors and a small radio transmitter. This unit requires no special writing pad.

Such signature-capture units don't, however, perform a function akin to that of voiceprint equipment attached to a telephone. Signature-capture units can't validate a signature already affixed to a document that you receive by mail or fax.



**Fingerprint sensing can add security to computer networks and the Internet. Digital Persona's \$99 USB-interfaced U.are.U optical fingerprint sensor is available with software that establishes a database of the fingerprints of legitimate network users. The software allows access only to enrolled users.**

## BIOMETRICS

If PCs are to be the first mass-market products to incorporate biometrics, a good place to start seems to be with notebook PCs. Compared with desktop units, notebooks are more subject to theft and tampering and have shorter useful lives. Today, most information-technology (IT) managers would probably pay a modest premium for an easy-to-use alternative to password protection of such machines. But many of these managers expect to wait several years before they consider widespread deployment of biometrics on desktop PCs and workstations.

As with any ascendant computer technology, standards and software must precede ubiquitous deployment. Moreover, the largest purchasers of the new technology—IT managers in medium and large companies—must convince themselves of a reasonable pay back. Although some devices, such as IC fingerprint sensors, may eventually cost less than \$5 in quantity, the total cost of installing biometric sensing is several times the sensing unit's cost. Moreover, much of the initial crop of sensing units uses USB interfaces. As a result, biometric sensing on PCs may become cost-effective only when IT managers replace the installed base of computers with USB-compliant PCs.

Because of the structure of the computer industry, making biometric security a feature of embedded systems—cellular phones, for example—may be simpler than adding similar features to PCs. Unlike the PC, the cell phone is a fixed-purpose device. To successfully incorporate biometrics, cell-phone developers need not gather support from nearly as many groups as PC-application developers must.

Before they can begin widespread product deployment, developers of PC biometric products must wait for representatives of dozens of companies to work out the details of a generalized biometric application-programming interface (API). This work requires the cooperation of BIOS vendors,

the operating-system vendor, add-on security-hardware vendors, and developers of applications that must recognize the security features. Currently in the computer industry, at least four efforts are under way to develop biometric APIs.

**Made for just embedded systems**

The situation in embedded applications differs somewhat. In many cases, embedded applications cry out for ways to improve security without encumbering users with complex procedures. For example, biometrics sometimes permits eliminating cards, such as those that restrict workplace access to small groups of employees. Moreover, controlling access does not involve remembering PINs or passwords.

Cellular phones are one type of embedded system whose ease-of-use requirements, large production volumes, and vulnerability to theft make them strong contenders for biometrics. Cell phones need improved security to prevent their unauthorized use. Over the next five years, millions of North American cellular subscribers will replace their phones as they upgrade to

digital cellular technology. This mass upgrade appears to offer biometrics advocates a golden opportunity for widespread deployment of their technology in compact, moderately priced products. Despite this opportunity, however, many biometrics companies seem determined not to be distracted from a PC focus.

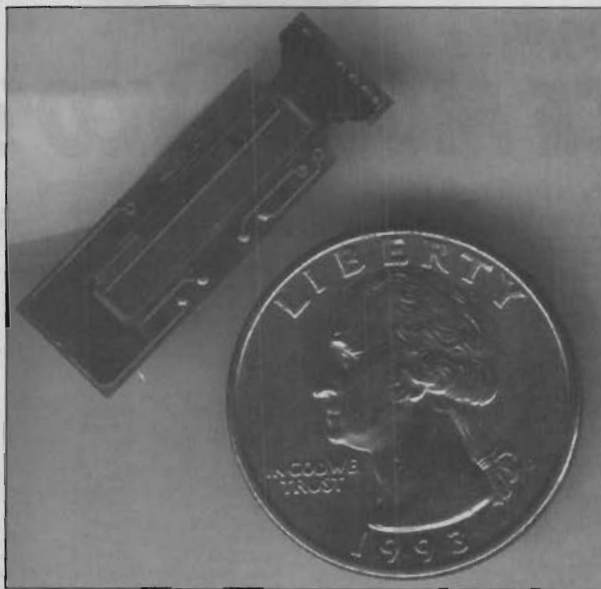
Adding biometric security to a cell phone is hardly trivial. However, surmounting the challenges—maintaining small size and weight and low power consumption—should produce a substantial payoff. The miniaturization that cell phones require should help make biometric technology more widely acceptable.

**Deciding which is best**

Just which biometric technologies are best for particular applications has become the subject of heated debates. Fueling the fervor is the lack of objective information comparing the accuracy of the various technologies. Factors that add interest to the comparison include the ease of use, the likelihood of public acceptance, and the ease with which someone intent on deception can fool a technique.

The two technologies that probably offer the highest accuracy are iris scans and facial thermal imaging. Until recently, iris scans were inconvenient; they required the subject to hold still and look directly at the camera. Most people instinctively averted their gaze. Improved technology uses multiple cameras and high-speed real-time video processing to overcome these problems (Reference 1). Both thermal imaging and iris scanning are among the most expensive biometric-authentication technologies. An iris-scanning station costs about \$5000. Costs for thermal imaging are harder to pin down but appear to be comparable.

The drastic drop in the price of desktop videocameras has led to widespread deployment of the devices, some of which are now part of video monitors



**The FingerChip IC fingerprint sensor from Thomson-CSF uses thermal sensing. Unlike other IC fingerprint sensors, the device need not be as large as your finger tip, because you draw your finger across the 2-D sensor array. According to the company, the speed at which you move your finger is not critical—as it was in earlier versions that used a 1-D sensor array.**

## BIOMETRICS

(Reference 2). This widespread deployment has prompted companies such as Miro, Visionics, and Viisage to develop authentication systems based on monitoring the images these cameras produce. The systems claim to detect impostors, and the companies have videos that show the systems doing just that. Despite these demos, potential users continue to express some skepticism about facial-imaging accuracy.

To allay such doubts, some companies, such as Qvoice, combine multiple technologies. Every PC that comes with a video camera also contains a sound card, and nearly every sound card has a microphone input. The audio input is thus, in effect, a no-cost feature that biometrics-software companies can harness to offer improved security.

Of course, an impostor, disguised as you, might connect a tape recorder to the sound card's microphone input and play back a recording of your voice. The voice-recognition software probably couldn't distinguish the recording from the real thing. However, the software could work around this deficiency by requiring the subject to repeat a phrase the computer randomly selects from a large repertoire. In all likelihood, an impostor would be unable to get a recorder to play back the correct phrase within a prescribed period.

### Likelihood is the key

The issue of likelihood is central to discussions of biometrics. No system can be 100%-accurate. The goal is to make fooling the system so complex and expensive that would-be attackers decide that the potential rewards don't justify the required effort. Still, the idea of combining multiple biometric technologies into one system is at the heart of another debate among biometrics advocates. Some—particularly those who advocate the use of fingerprint sensing—assert that one technology is enough. The fingerprint advocates point out that most people have 10 fingerprints. If one print can verify your identity with a 1% error, using two prints should result in a 0.01% error.

Still, none of the systems is perfect. Fingerprint sensors have had a reputation for being subject to errors from

latent prints—those left by the previous subject. Optical fingerprint sensors are probably more subject to this problem than are some newer types, such as capacitive and thermal devices. Fingerprint sensing also encounters difficulties in areas such as construction sites and machine shops, where many subjects' fingers are dirty, cut, or deeply callused. Such fingers do not produce good images and system accuracy suffers. Alternatives that overcome these problems (but introduce new issues) include scanning of the palm of the hand or measuring the geometry of the entire hand.

Despite its problems, biometric security offers several advantages over current approaches. People can steal or copy keys. Badges used to control admission to secure areas are of no value unless they require you to enter a PIN. You can too easily forget your password or PIN, and if you write it down, someone else may find it and misuse it.

Sales clerks rarely seem to check whether your signature matches the signature on the back of your credit card. The airport ticket agent's check of the photo on your driver's license or passport is the only type of identity check that appears to be more than perfunctory. Yet, even this check is far from foolproof. Moreover, men who grow or shave off mustaches and beards and women who change their hair style or hair color sometimes have to get new photo IDs—a real nuisance.

### Biometrics—not always better

Despite the problems with conventional approaches, biometric approaches are not always better. In many cases, the people who propose using biometrics do not appear to have thought



**By placing a fingerprint sensor in your PC's keyboard, Who? Vision Systems does not require you to have a PC that supports USB or to share the printer port with other peripherals. The company says that adding the fingerprint sensor costs keyboard manufacturers only \$25 to \$50 per unit.**

through the host of details that can make or break an application.

For example, although a fingerprint reader might work well at your local supermarket or discount department store, how would it work in a restaurant? Would you have to go to the cashier instead of paying the server? Although you might welcome never having your credit card leave your sight, this procedure doesn't seem to fit well with the ambiance of even moderately priced restaurants. Maybe the server would bring a special cellular phone/modem/card reader and fingerprint reader to your table. If so, how many customers would object to being fingerprinted to pay a restaurant tab? If fingerprint recognition turns out to be unacceptable in restaurants, would other types of retail businesses accept the technology?

Widespread use of biometrics for identification would noticeably affect most people's lives. Unless people perceive the changes as unintrusive or innocuous or as a great improvement over the "old way," a public outcry is likely. Should public opposition emerge, all sorts of scary stories and urban legends will proliferate. Already, you may have heard the question, "Would you want your fingerprints



## BIOMETRICS

floating all over the Internet?" This question suggests that such files would be unprotected. In fact, fingerprints will be automatically encrypted, usually by a processor within the sensing unit or associated PC. Encryption limits access to the intended recipient (Reference 3).

A vocal group, fearing loss of privacy and government control of their lives, is already up in arms over the expanding use of fingerprints and other biometric technology. One of the Web sites at which you can read about the group's concerns and activities is [www.networkusa.org/fingerprint.shtml](http://www.networkusa.org/fingerprint.shtml).

### Biometrics and smart cards

A technology that may well turn out to be closely linked to biometrics is smart-card technology (Reference 4). One of the ideas behind smart cards is to decrease the dependence on centralized databases for storing personal data. Magnetic-stripe cards, such as those currently popular in the United States, are not smart. Such cards may provide access to important personal data, but the data resides on a remote computer. You or someone else—a health-care provider, for example—can use the magnetic-stripe card to access the remote database.

Smart cards would remove some of the data that pertains to you from the centralized database. This data would reside on your card. Without protection, however, the data would be ripe for misuse. The protection would come in the form of encryption—possibly based on biometrics. For example, software that generates keys for a dual-key encryption system might use data derived from a biometric sensor, such as a fingerprint sensor, to generate one of the keys.

Legal issues will almost surely delay and complicate the introduction of biometrics into your daily routine. If society is to realize the technology's full potential, changes are necessary in many laws. For example, laws that require your signature or photograph on certain documents will have to allow (though probably not require) the substitution of biometric identity-verification techniques.

One way in which biometrics might fail is by setting people's expectations too high. No biometric technique is foolproof. People need to be clear on that issue. Getting objective comparisons of the false acceptance rate (FAR) and false rejection rate (FRR) of various technologies is just about impossible. The FAR is the percentage of time that a system grants access to someone who is misrepresenting himself. The FRR is the percentage of time that a system denies access to a legitimate applicant. In general, in any system, the more stringent you make the acceptance criteria, the lower the FAR becomes and the higher the FRR becomes.

In most biometric-security applications, you don't ask the system to determine the identity of the person who presents himself to the system. That is, you don't say to the system, "Of the millions of sets of fingerprints you have on file, which set contains a print that matches this print?" This problem is "one-to-many matching." Usually, you supply your identity to the system, often by presenting a machine-readable ID card, and ask the system to confirm that you are who you say you are. This problem is "one-to-one matching." Today's PCs can conduct a one-to-one match in, at most, a few seconds.

One-to-one matching differs significantly from one-to-many matching. In a system that stores a million sets of prints, a one-to-many match requires comparing the presented fingerprint with 10 million prints (1 million sets times 10 prints/set). One-to-many matching is typical of fingerprint searches that law-enforcement authorities conduct with the aid of automatic fingerprint-identification systems (AFISs). Some proposed iris-scan systems would also perform one-to-many matching, using only an iris scan to identify an individual.

AFISs are expensive (typically more than \$1 million) systems that incorporate high-speed parallel processors. The systems do not make the final judgment on which stored fingerprints match the presented print. Rather, the systems determine which sets of stored prints have a high likelihood of matching the presented print. Human experts

then further evaluate the AFIS selections to see which are most likely to match the presented print.

Biometric identity verification is almost always a case of one-to-one or one-to-a-few matching. At an ATM, for example, you would still have to present your card. But, instead of keying in your password, you would press your finger against a fingerprint sensor, speak a predetermined phrase into a microphone, or look at a videocamera.

An example of one-to-a-few matching is an entry-control system for the restricted-access work area of a small work group (of, say, 20 people or fewer). In this example, the workers might not need access cards; they might need to present only a fingerprint to a sensor at the point of entry. A modest computer could determine within a few seconds whether the presented print matched one of the prints in the 20 sets in the database. EDN

## References

1. Webb, Warren, "High-tech security: The eyes have it," *EDN*, Dec 18, 1997, pg 75.
2. Wright, Maury, "Digital-camera interfaces lead to ubiquitous deployment," *EDN*, Jan 15, 1998, pg 63.
3. Strassberg, Dan, "Data security: key issue in an age of pervasive computing," *EDN*, April 11, 1996, pg 48.
4. Gallant, John, "Smart cards... trained for security," *EDN*, Nov 23, 1995, pg 34.



You can reach Senior Technical Editor Dan Strassberg at 1-617-558-4205, fax 1-617-928-4205, [ednstrassberg@cahners.com](mailto:ednstrassberg@cahners.com).

**Turn to page 63 for a list of manufacturers of biometric products.**

## VOTE

Please use the Information Retrieval Service card to rate this article (circle one):

High  
Interest  
590

Medium  
Interest  
591

Low  
Interest  
592